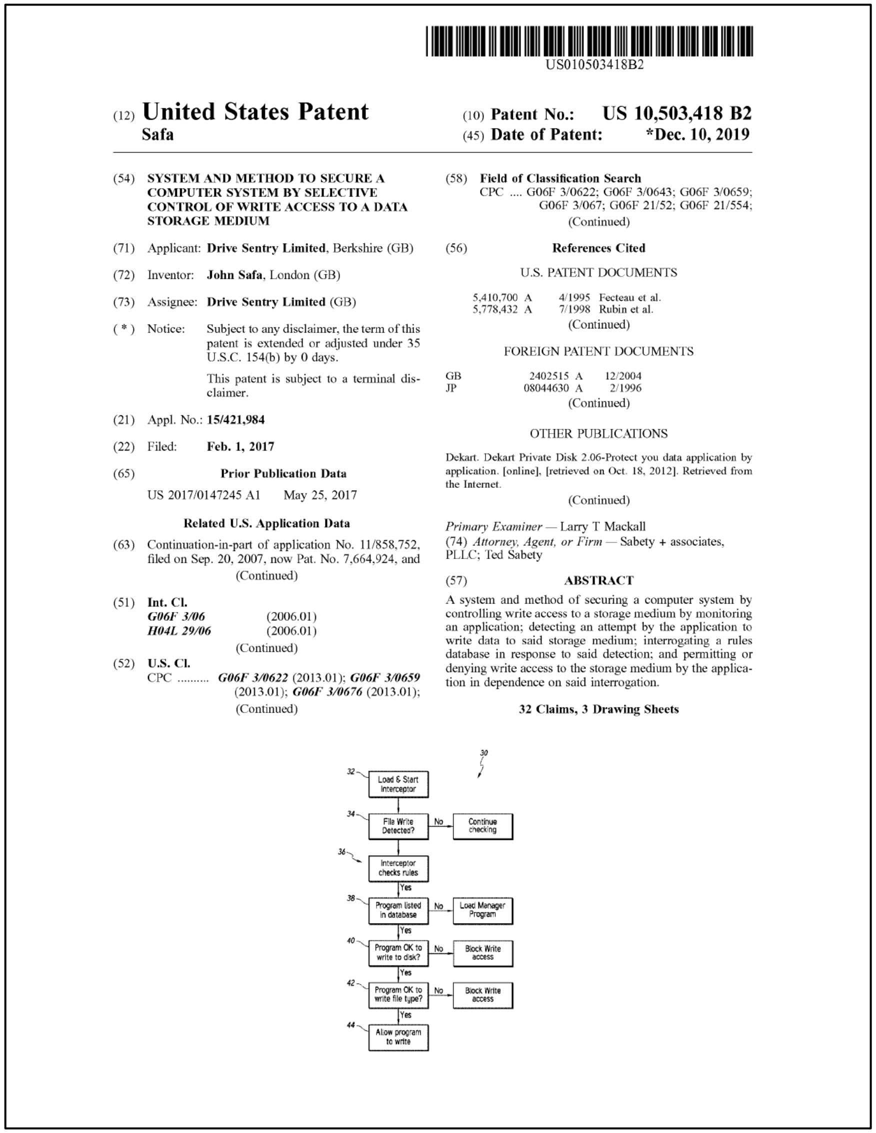
Ex. F - Claim Chart
U.S. Patent No. 10,503,418



US010503418B2

(12) **United States Patent**
Safa

(10) **Patent No.:** **US 10,503,418 B2**
(45) **Date of Patent:** ***Dec. 10, 2019**

(54) **SYSTEM AND METHOD TO SECURE A COMPUTER SYSTEM BY SELECTIVE CONTROL OF WRITE ACCESS TO A DATA STORAGE MEDIUM**

(71) Applicant: **Drive Sentry Limited**, Berkshire (GB)

(72) Inventor: **John Safa**, London (GB)

(73) Assignee: **Drive Sentry Limited** (GB)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/421,984**

(22) Filed: **Feb. 1, 2017**

(65) **Prior Publication Data**

US 2017/0147245 A1 May 25, 2017

Related U.S. Application Data

(63) Continuation-in-part of application No. 11/858,752, filed on Sep. 20, 2007, now Pat. No. 7,664,924, and

(Continued)

(51) **Int. Cl.**
G06F 3/06 (2006.01)
H04L 29/06 (2006.01)

(Continued)

(52) **U.S. Cl.**
CPC ***G06F 3/0622*** (2013.01); ***G06F 3/0659*** (2013.01); ***G06F 3/0676*** (2013.01);

(Continued)

(58) **Field of Classification Search**
CPC G06F 3/0622; G06F 3/0643; G06F 3/0659; G06F 3/067; G06F 21/52; G06F 21/554;

(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,410,700	A	4/1995	Fecteau et al.
5,778,432	A	7/1998	Rubin et al.

(Continued)

FOREIGN PATENT DOCUMENTS

GB	2402515	A	12/2004
JP	08044630	A	2/1996

(Continued)

OTHER PUBLICATIONS

Dekart. Dekart Private Disk 2.06-Protect you data application by application. [online], [retrieved on Oct. 18, 2012]. Retrieved from the Internet.

(Continued)

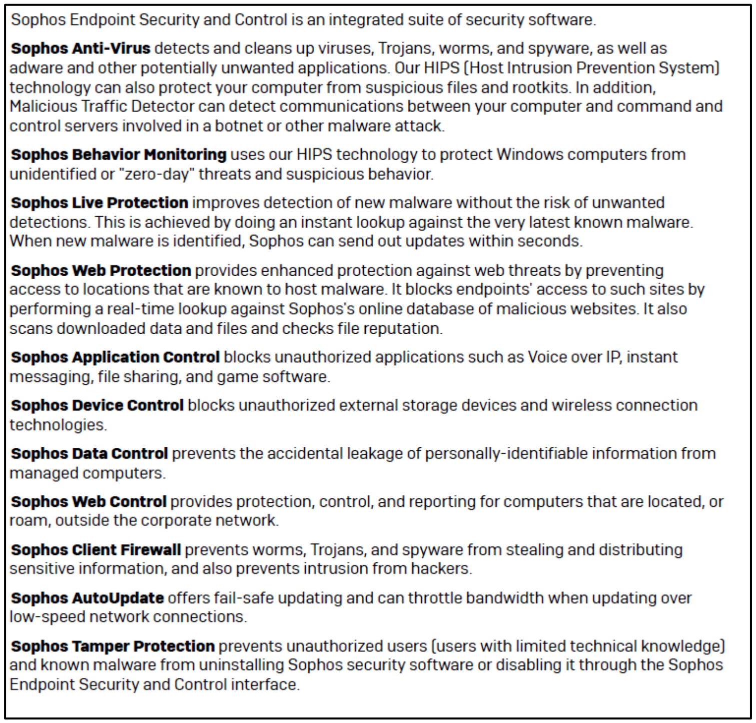
Primary Examiner — Larry T Mackall
(74) *Attorney, Agent, or Firm* — Sabety + associates, PLLC; Ted Sabety

(57) **ABSTRACT**

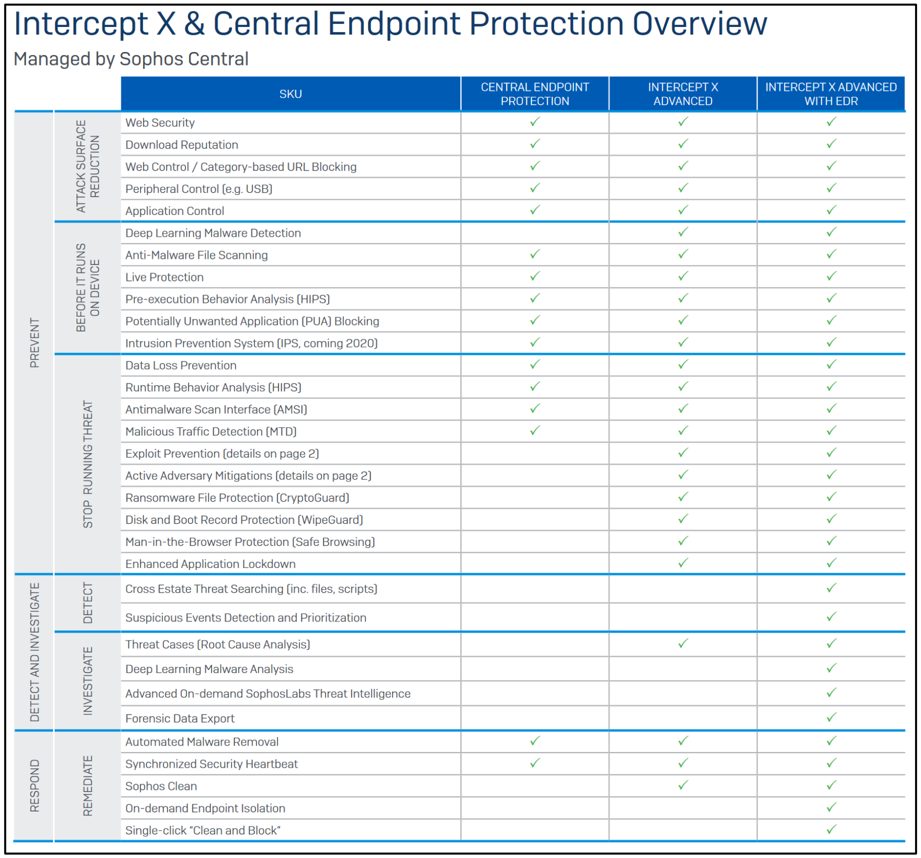
A system and method of securing a computer system by controlling write access to a storage medium by monitoring an application; detecting an attempt by the application to write data to said storage medium; interrogating a rules database in response to said detection; and permitting or denying write access to the storage medium by the application in dependence on said interrogation.

32 Claims, 3 Drawing Sheets

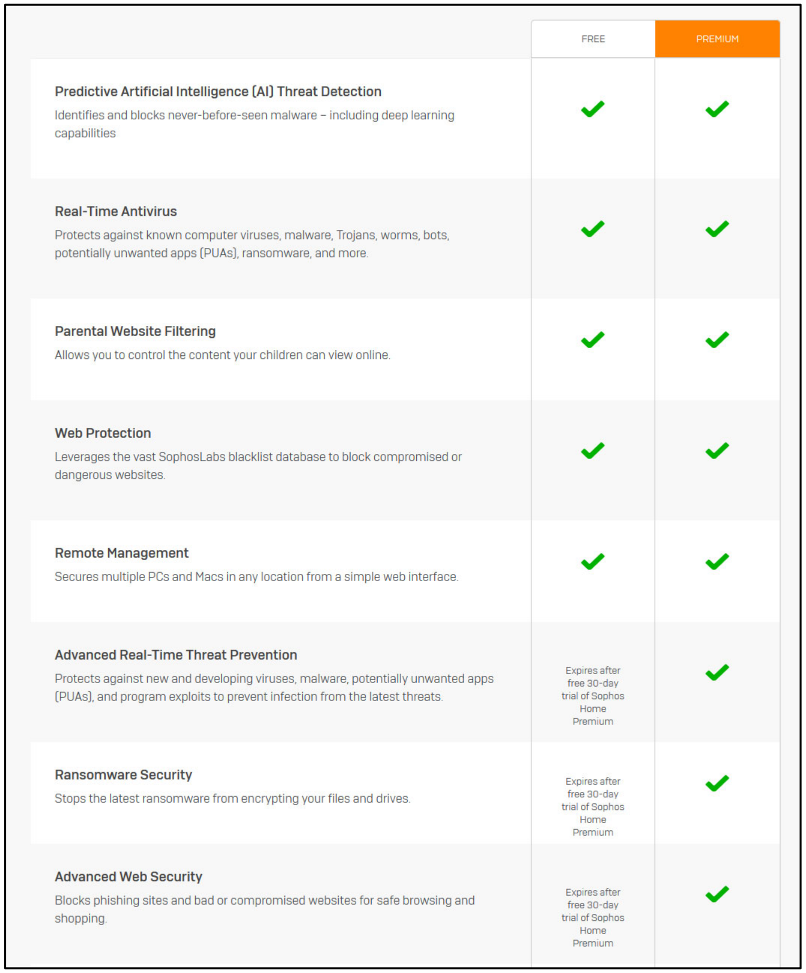
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[pre] A method of controlling write access to a data storage device by an application running in application space on a first computer comprising:	Sophos performs the method of claim 29 via its SophosLabs network. Specifically, Sophos offers many products that can run on endpoints or end-user devices (i.e., on a first computer) to protect those devices from electronic threats such as viruses, ransomware, malware, and the like (collectively “hostile applications”). That software includes but is not limited to, software that includes, Sophos Anti-Virus, Sophos Behavior Monitoring, and/or Sophos Live Protection. For example, the infringing products include Endpoint Security and Control, Intercept X, Intercept X Advanced, Intercept X Advanced with EDR, Central Endpoint Protection, Home, and Home Premium.  Sophos Endpoint Security and Control is an integrated suite of security software. **Sophos Anti-Virus** detects and cleans up viruses, Trojans, worms, and spyware, as well as adware and other potentially unwanted applications. Our HIPS (Host Intrusion Prevention System) technology can also protect your computer from suspicious files and rootkits. In addition, Malicious Traffic Detector can detect communications between your computer and command and control servers involved in a botnet or other malware attack. **Sophos Behavior Monitoring** uses our HIPS technology to protect Windows computers from unidentified or "zero-day" threats and suspicious behavior. **Sophos Live Protection** improves detection of new malware without the risk of unwanted detections. This is achieved by doing an instant lookup against the very latest known malware. When new malware is identified, Sophos can send out updates within seconds. **Sophos Web Protection** provides enhanced protection against web threats by preventing access to locations that are known to host malware. It blocks endpoints' access to such sites by performing a real-time lookup against Sophos's online database of malicious websites. It also scans downloaded data and files and checks file reputation. **Sophos Application Control** blocks unauthorized applications such as Voice over IP, instant messaging, file sharing, and game software. **Sophos Device Control** blocks unauthorized external storage devices and wireless connection technologies. **Sophos Data Control** prevents the accidental leakage of personally-identifiable information from managed computers. **Sophos Web Control** provides protection, control, and reporting for computers that are located, or roam, outside the corporate network. **Sophos Client Firewall** prevents worms, Trojans, and spyware from stealing and distributing sensitive information, and also prevents intrusion from hackers. **Sophos AutoUpdate** offers fail-safe updating and can throttle bandwidth when updating over low-speed network connections. **Sophos Tamper Protection** prevents unauthorized users (users with limited technical knowledge) and known malware from uninstalling Sophos security software or disabling it through the Sophos Endpoint Security and Control interface. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf, at p. 2

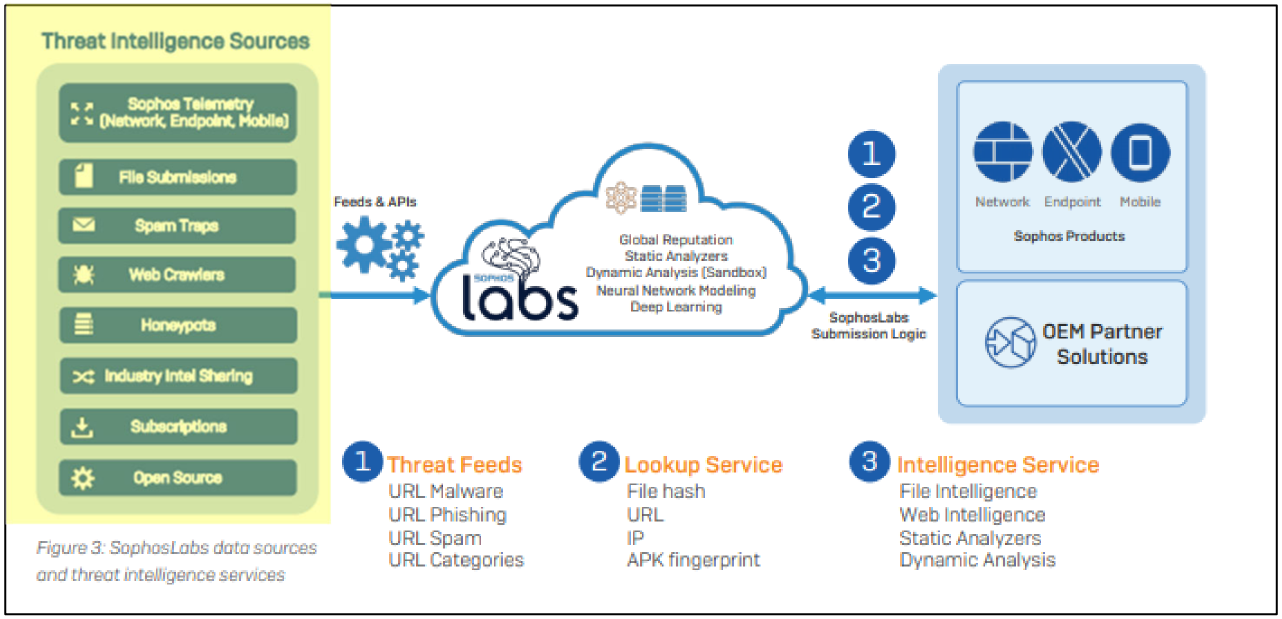
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

<table>
<tr><th>CLAIM 29</th><th>SOPHOS PRODUCTS</th></tr>
<tr><td><b>29[pre] A method of controlling write access to a data storage device by an application running in application space on a first computer comprising:</b></td><td>Relevant features discussed in this chart span the software of Endpoint Security and Control, Intercept X, Intercept X Advanced, Intercept X Advanced with EDR, Central Endpoint, Home, and Home Premium as shown in this charts. Upon information and belief, Endpoint Security and Control is an earlier iteration of the Intercept X & Central Endpoint Suite.

Intercept X & Central Endpoint Protection Overview
Managed by Sophos Central
<table>
<tr><th></th><th></th><th>SKU</th><th>CENTRAL ENDPOINT PROTECTION</th><th>INTERCEPT X ADVANCED</th><th>INTERCEPT X ADVANCED WITH EDR</th></tr>
<tr><td>PREVENT</td><td>ATTACK SURFACE REDUCTION</td><td>Web Security</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Download Reputation</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Web Control / Category-based URL Blocking</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Peripheral Control (e.g. USB)</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Application Control</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td>BEFORE IT RUNS ON DEVICE</td><td>Deep Learning Malware Detection</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Anti-Malware File Scanning</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Live Protection</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Pre-execution Behavior Analysis (HIPS)</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Potentially Unwanted Application (PUA) Blocking</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Intrusion Prevention System (IPS, coming 2020)</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td>STOP RUNNING THREAT</td><td>Data Loss Prevention</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Runtime Behavior Analysis (HIPS)</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Antimalware Scan Interface (AMSI)</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Malicious Traffic Detection (MTD)</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Exploit Prevention (details on page 2)</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Active Adversary Mitigations (details on page 2)</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Ransomware File Protection (CryptoGuard)</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Disk and Boot Record Protection (WipeGuard)</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Man-in-the-Browser Protection (Safe Browsing)</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Enhanced Application Lockdown</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td>DETECT AND INVESTIGATE</td><td>DETECT</td><td>Cross Estate Threat Searching (inc. files, scripts)</td><td></td><td></td><td>✓</td></tr>
<tr><td></td><td></td><td>Suspicious Events Detection and Prioritization</td><td></td><td></td><td>✓</td></tr>
<tr><td></td><td>INVESTIGATE</td><td>Threat Cases (Root Cause Analysis)</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Deep Learning Malware Analysis</td><td></td><td></td><td>✓</td></tr>
<tr><td></td><td></td><td>Advanced On-demand SophosLabs Threat Intelligence</td><td></td><td></td><td>✓</td></tr>
<tr><td></td><td></td><td>Forensic Data Export</td><td></td><td></td><td>✓</td></tr>
<tr><td>RESPOND</td><td>REMEDIATE</td><td>Automated Malware Removal</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Synchronized Security Heartbeat</td><td>✓</td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>Sophos Clean</td><td></td><td>✓</td><td>✓</td></tr>
<tr><td></td><td></td><td>On-demand Endpoint Isolation</td><td></td><td></td><td>✓</td></tr>
<tr><td></td><td></td><td>Single-click “Clean and Block”</td><td></td><td></td><td>✓</td></tr>
</table>
https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophos-endpoint-license-guide.pdf</td></tr>
</table>

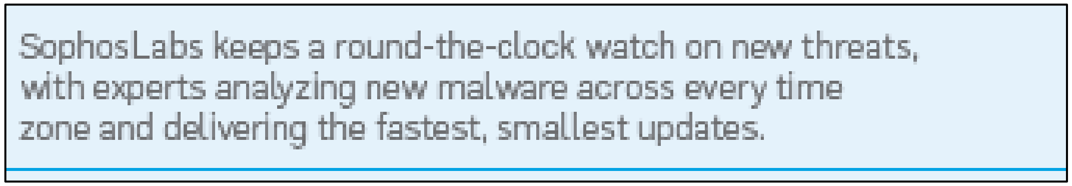
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

<table>
<tr><th>CLAIM 29</th><th>SOPHOS PRODUCTS</th></tr>
<tr><td><b>29[pre] A method of controlling write access to a data storage device by an application running in application space on a first computer comprising:</b></td><td>This chart shows an overview of the Sophos Home and Home Premium editions.

<table>
<tr><th></th><th>FREE</th><th>PREMIUM</th></tr>
<tr><td><b>Predictive Artificial Intelligence (AI) Threat Detection</b>
Identifies and blocks never-before-seen malware – including deep learning capabilities</td><td>✓</td><td>✓</td></tr>
<tr><td><b>Real-Time Antivirus</b>
Protects against known computer viruses, malware, Trojans, worms, bots, potentially unwanted apps (PUAs), ransomware, and more.</td><td>✓</td><td>✓</td></tr>
<tr><td><b>Parental Website Filtering</b>
Allows you to control the content your children can view online.</td><td>✓</td><td>✓</td></tr>
<tr><td><b>Web Protection</b>
Leverages the vast SophosLabs blacklist database to block compromised or dangerous websites.</td><td>✓</td><td>✓</td></tr>
<tr><td><b>Remote Management</b>
Secures multiple PCs and Macs in any location from a simple web interface.</td><td>✓</td><td>✓</td></tr>
<tr><td><b>Advanced Real-Time Threat Prevention</b>
Protects against new and developing viruses, malware, potentially unwanted apps (PUAs), and program exploits to prevent infection from the latest threats.</td><td>Expires after free 30-day trial of Sophos Home Premium</td><td>✓</td></tr>
<tr><td><b>Ransomware Security</b>
Stops the latest ransomware from encrypting your files and drives.</td><td>Expires after free 30-day trial of Sophos Home Premium</td><td>✓</td></tr>
<tr><td><b>Advanced Web Security</b>
Blocks phishing sites and bad or compromised websites for safe browsing and shopping.</td><td>Expires after free 30-day trial of Sophos Home Premium</td><td>✓</td></tr>
</table>
https://home.sophos.com/en-us/free-anti-virus-windows.aspx</td></tr>
</table>

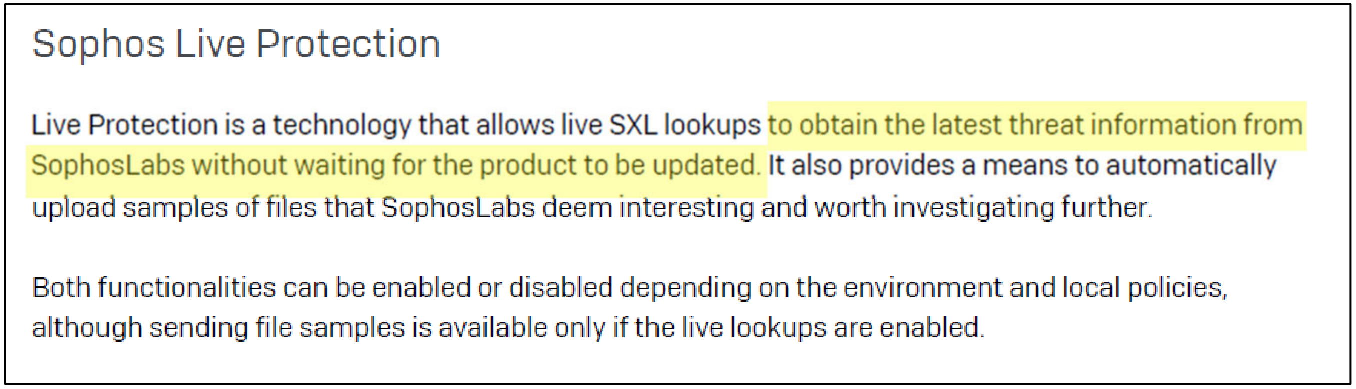
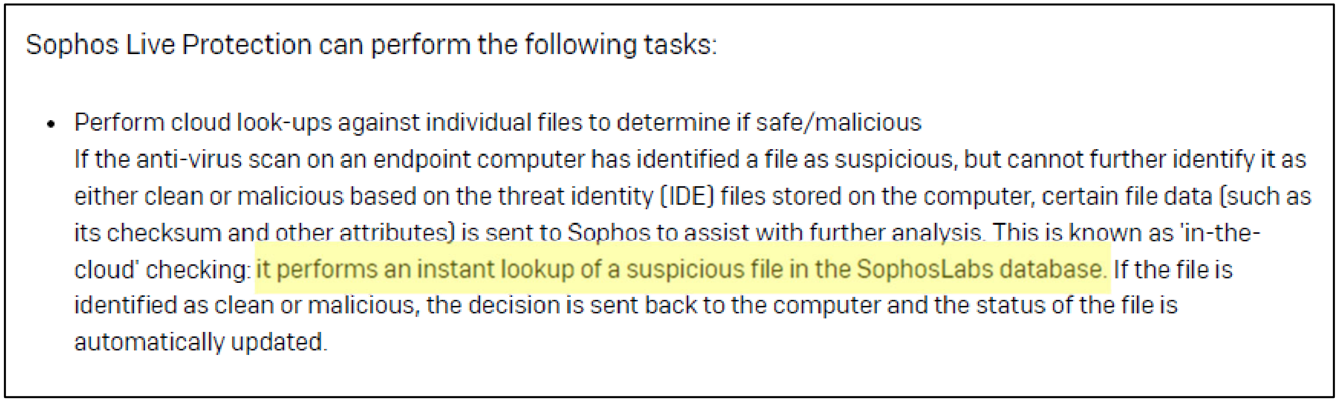
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

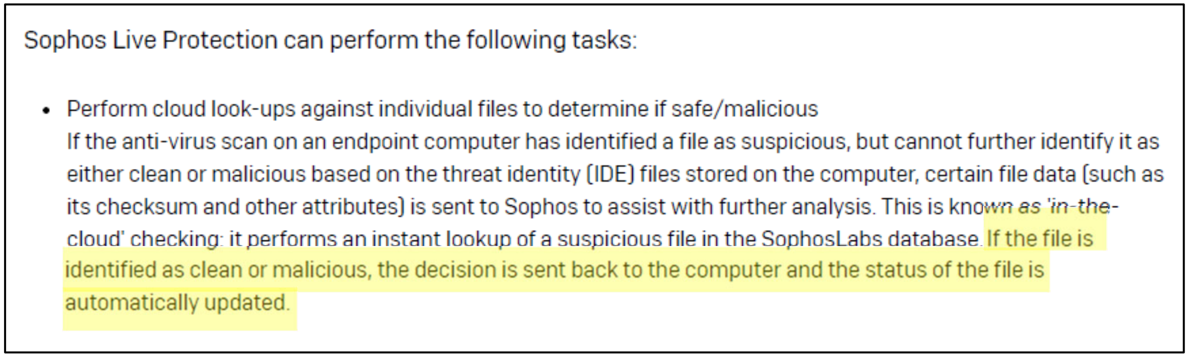
CLAIM 29	SOPHOS PRODUCTS
29[a] receiving at a server computer from a plurality second computers operatively connected to the server by means of a data network, a corresponding plurality of permission values associated with the application operating on the first computer;	The SophosLabs network receives at a server computer from a plurality second computers operatively connected to the server by means of a data network, a corresponding plurality of permission values associated with the application operating on the first computer. The SophosLabs network includes servers that collect data via a data network from many resources that comprise a plurality of second computers, including the “Threat Intelligence Sources” shown below. Those permission values can be, for example, allowing the application access, denying the application access, and/or a whitelist value.  Threat Intelligence Sources Sophos Telemetry (Network, Endpoint, Mobile) File Submissions Spam Traps Web Crawlers Honeypots Industry Intel Sharing Subscriptions Open Source Feeds & APIs SOPHOS labs Global Reputation Static Analyzers Dynamic Analysis (Sandbox) Neural Network Modeling Deep Learning 1 2 3 SophosLabs Submission Logic Network Endpoint Mobile Sophos Products OEM Partner Solutions 1 Threat Feeds URL Malware URL Phishing URL Spam URL Categories 2 Lookup Service File hash URL IP APK fingerprint 3 Intelligence Service File Intelligence Web Intelligence Static Analyzers Dynamic Analysis *Figure 3: SophosLabs data sources and threat intelligence services* https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/oem-solutions/sophos-threat-intelligence-dsna.pdf, at p. 3

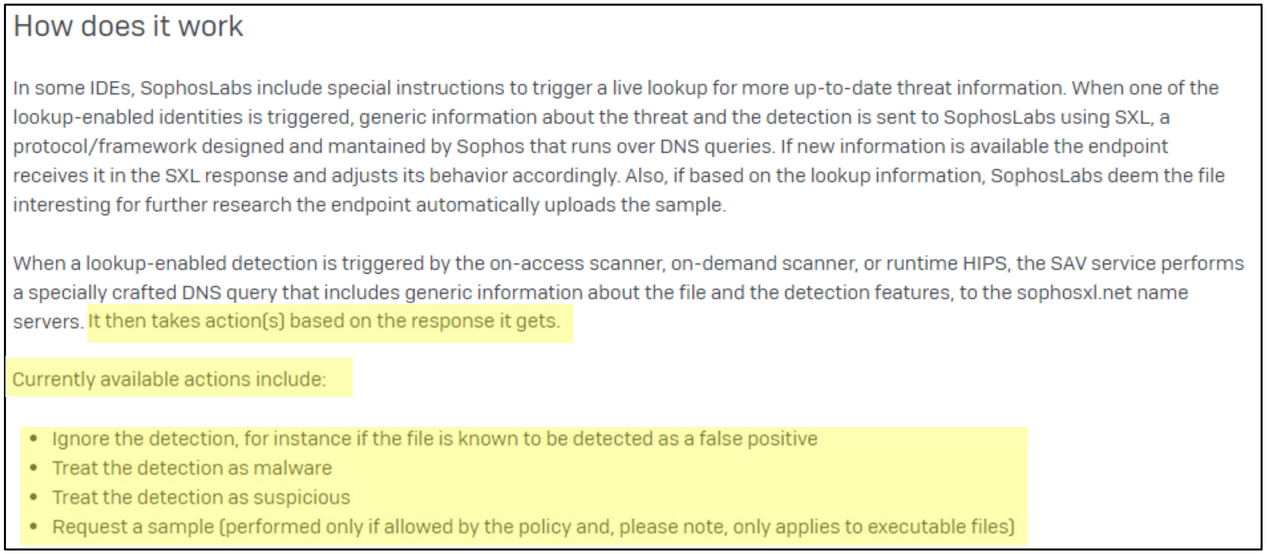
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[a] receiving at a server computer from a plurality second computers operatively connected to the server by means of a data network, a corresponding plurality of permission values associated with the application operating on the first computer;	As another example, the SophosLabs network is operatively connected to second computers associated with Sophos's agents (e.g., experts) who analyze malware and provide updates to the server based on the analysis.  SophosLabs keeps a round-the-clock watch on new threats, with experts analyzing new malware across every time zone and delivering the fastest, smallest updates. https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/sophosendpointsecurityanddataprotectionrgna.pdf, at p. 14

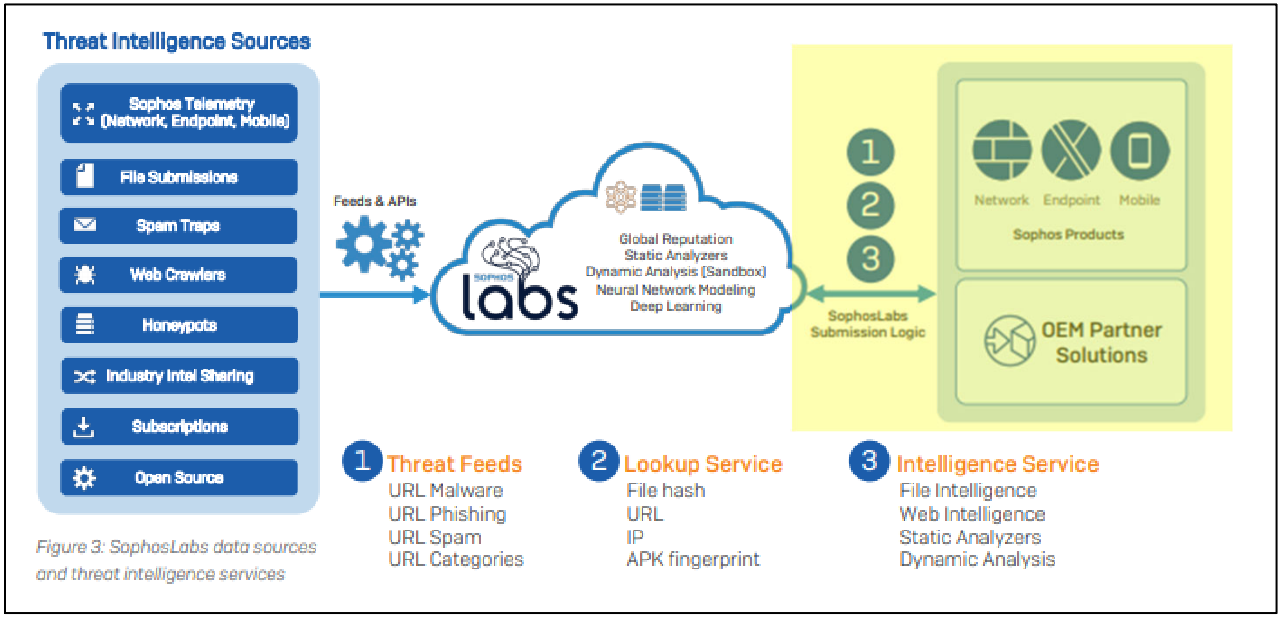
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[b] storing said permission values;	The SophosLabs network stores the permission values so that it can maintain the latest threat information based on, at least in part, the second computers discussed in the slides relating to element 29[a].  Sophos Live Protection Live Protection is a technology that allows live SXL lookups to obtain the latest threat information from SophosLabs without waiting for the product to be updated. It also provides a means to automatically upload samples of files that SophosLabs deem interesting and worth investigating further. Both functionalities can be enabled or disabled depending on the environment and local policies, although sending file samples is available only if the live lookups are enabled. https://community.sophos.com/kb/en-us/111334  Sophos Live Protection can perform the following tasks: • Perform cloud look-ups against individual files to determine if safe/malicious If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis. This is known as 'in-the-cloud' checking: it performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated. https://community.sophos.com/kb/en-us/110921

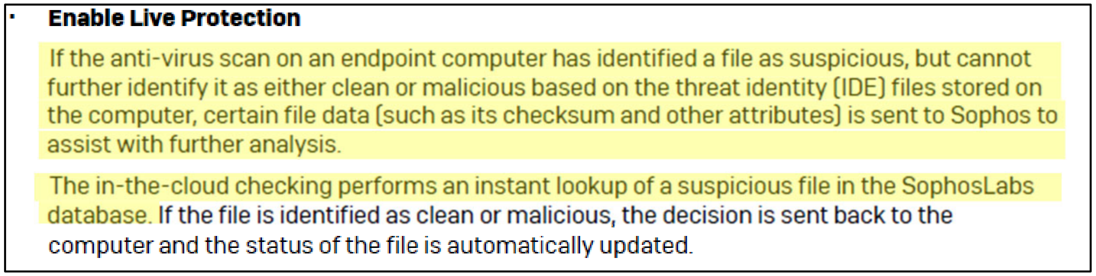
CLAIM 29	SOPHOS PRODUCTS
29[c] generating an output permission value for the application in dependence on the stored permission values;	The SophosLabs network generates an output permission value for the application in dependence on the stored permission values. For example, the stored permission values indicate whether an application is clean or malicious and the SophosLabs network generates an output permissive value that is sent back to the computer.  Sophos Live Protection can perform the following tasks: - Perform cloud look-ups against individual files to determine if safe/malicious If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis. This is known as 'in-the-cloud' checking: it performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated. https://community.sophos.com/kb/en-us/110921

CLAIM 29	SOPHOS PRODUCTS
29[c] generating an output permission value for the application in dependence on the stored permission values;	As another example, the stored permission value may indicate whether to ignore the application, treat the application as malware, or treat the detection as suspicious. The SophosLabs network generates an output permissive value that is sent back to the computer to indicate available actions based on the stored permission value.  How does it work In some IDEs, SophosLabs include special instructions to trigger a live lookup for more up-to-date threat information. When one of the lookup-enabled identities is triggered, generic information about the threat and the detection is sent to SophosLabs using SXL, a protocol/framework designed and mantained by Sophos that runs over DNS queries. If new information is available the endpoint receives it in the SXL response and adjusts its behavior accordingly. Also, if based on the lookup information, SophosLabs deem the file interesting for further research the endpoint automatically uploads the sample. When a lookup-enabled detection is triggered by the on-access scanner, on-demand scanner, or runtime HIPS, the SAV service performs a specially crafted DNS query that includes generic information about the file and the detection features, to the sophosxl.net name servers. It then takes action(s) based on the response it gets. Currently available actions include: • Ignore the detection, for instance if the file is known to be detected as a false positive • Treat the detection as malware • Treat the detection as suspicious • Request a sample (performed only if allowed by the policy and, please note, only applies to executable files) https://community.sophos.com/kb/en-us/111334

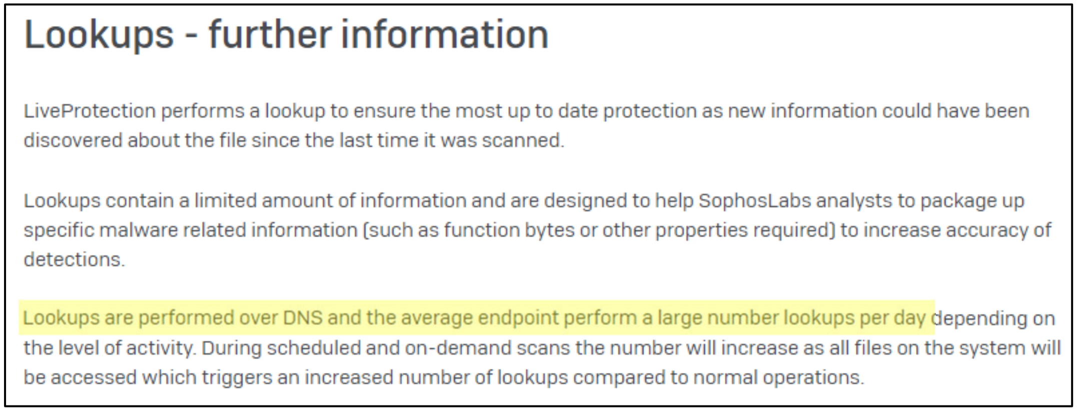
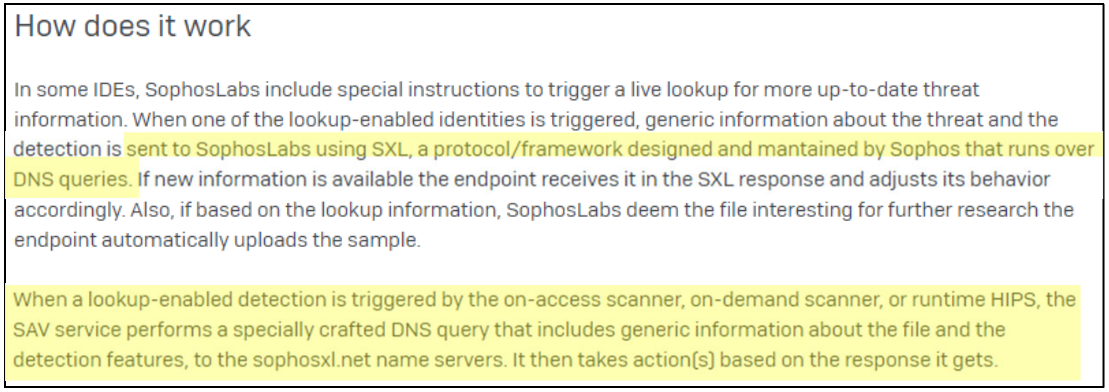
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The SophosLabs network servers receive at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application. The computer using Sophos's software (e.g., an endpoint) is operatively connected to SophosLabs network servers by means of a data network as shown below.  Threat Intelligence Sources Sophos Telemetry (Network, Endpoint, Mobile) File Submissions Spam Traps Web Crawlers Honeypots Industry Intel Sharing Subscriptions Open Source Feeds & APIs SOPHOS labs Global Reputation Static Analyzers Dynamic Analysis (Sandbox) Neural Network Modeling Deep Learning 1 2 3 SophosLabs Submission Logic Network Endpoint Mobile Sophos Products OEM Partner Solutions 1 Threat Feeds URL Malware URL Phishing URL Spam URL Categories 2 Lookup Service File hash URL IP APK fingerprint 3 Intelligence Service File Intelligence Web Intelligence Static Analyzers Dynamic Analysis *Figure 3: SophosLabs data sources and threat intelligence services* https://www.sophos.com/en-us/medialibrary/pdfs/factsheets/oem-solutions/sophos-threat-intelligence-dsna.pdf, at p. 3

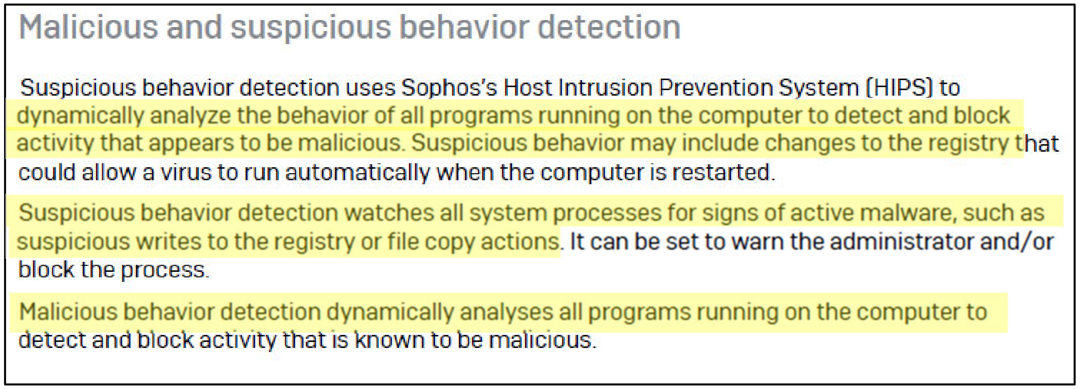
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The computer using Sophos's software sends a query that is received at a SophosLabs server as a request for a permission value associated with the application running on the first computer.  ▪ **Enable Live Protection** If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis. The in-the-cloud checking performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf, at p. 28

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	More specifically, the computer using Sophos's software sends, for example a DNS query to the SophosLabs server.  Lookups - further information LiveProtection performs a lookup to ensure the most up to date protection as new information could have been discovered about the file since the last time it was scanned. Lookups contain a limited amount of information and are designed to help SophosLabs analysts to package up specific malware related information (such as function bytes or other properties required) to increase accuracy of detections. Lookups are performed over DNS and the average endpoint perform a large number lookups per day depending on the level of activity. During scheduled and on-demand scans the number will increase as all files on the system will be accessed which triggers an increased number of lookups compared to normal operations. https://community.sophos.com/kb/en-us/110921  How does it work In some IDEs, SophosLabs include special instructions to trigger a live lookup for more up-to-date threat information. When one of the lookup-enabled identities is triggered, generic information about the threat and the detection is sent to SophosLabs using SXL, a protocol/framework designed and mantained by Sophos that runs over DNS queries. If new information is available the endpoint receives it in the SXL response and adjusts its behavior accordingly. Also, if based on the lookup information, SophosLabs deem the file interesting for further research the endpoint automatically uploads the sample. When a lookup-enabled detection is triggered by the on-access scanner, on-demand scanner, or runtime HIPS, the SAV service performs a specially crafted DNS query that includes generic information about the file and the detection features, to the sophosxl.net name servers. It then takes action(s) based on the response it gets. https://community.sophos.com/kb/en-us/111334

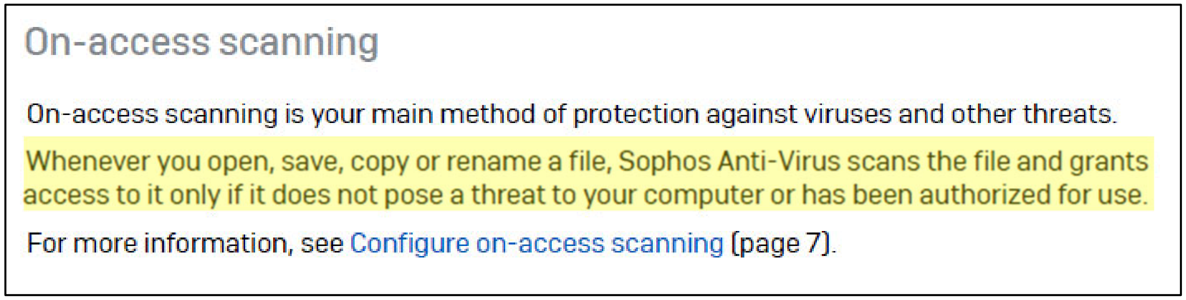
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The computer using Sophos's software sends a request (e.g., a Live Protection lookup query) in response to that software monitoring write access requests attempts by the application and detecting an attempt by the application to write data to a storage device (e.g., hard drive or memory) on the computer. For example, Sophos's "malicious behavior detection" analyzes programs running on the computer to detect and block known malicious activity, including attempts to write data to the data storage medium. As shown below, using Sophos's Behavior Monitoring, Sophos's "suspicious behavior detection analyzes the behavior of program and watches for signs of malware, such as suspicious writes to the registry or file copy actions."  Malicious and suspicious behavior detection Suspicious behavior detection uses Sophos's Host Intrusion Prevention System (HIPS) to dynamically analyze the behavior of all programs running on the computer to detect and block activity that appears to be malicious. Suspicious behavior may include changes to the registry that could allow a virus to run automatically when the computer is restarted. Suspicious behavior detection watches all system processes for signs of active malware, such as suspicious writes to the registry or file copy actions. It can be set to warn the administrator and/or block the process. Malicious behavior detection dynamically analyses all programs running on the computer to detect and block activity that is known to be malicious. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf, at pp. 25-26

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

<table>
<tr><th>CLAIM 29</th><th>SOPHOS PRODUCTS</th></tr>
<tr><td><b>29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;</b></td><td>

As another example, Sophos “on-access scanning,” detects attempts by the application to write data to said storage medium. For example, on-access scanning detects any attempts to open, save, copy or rename a file, which necessarily includes an attempt by the application to write data to said storage medium. Further, “on-access scanning” may be set to “check files on write.”

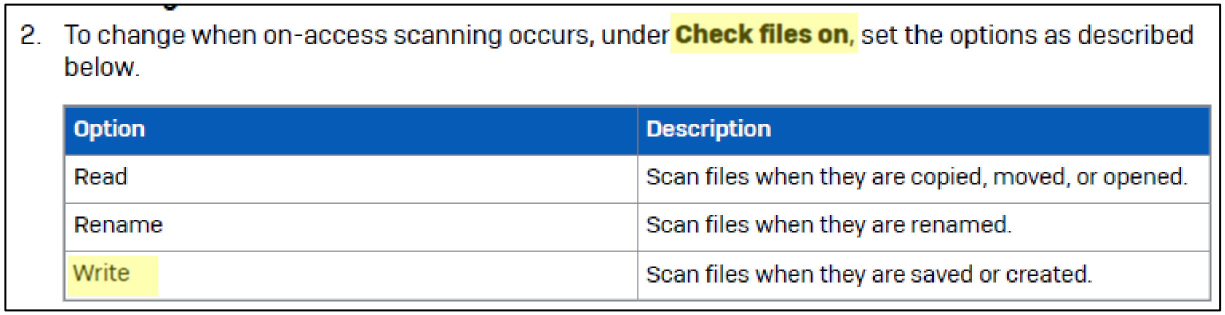


On-access scanning

On-access scanning is your main method of protection against viruses and other threats.

Whenever you open, save, copy or rename a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your computer or has been authorized for use.

For more information, see Configure on-access scanning (page 7).



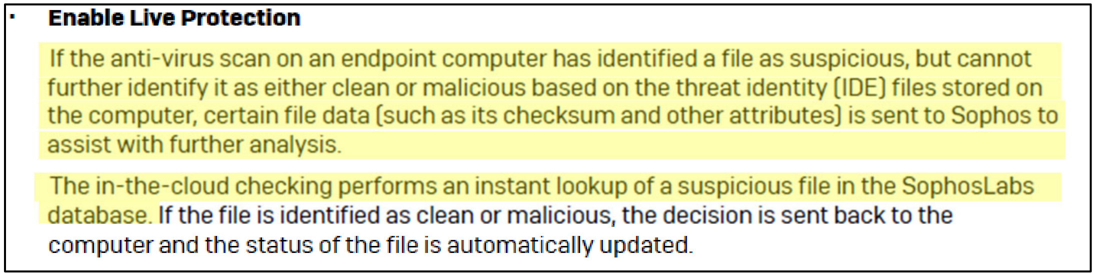
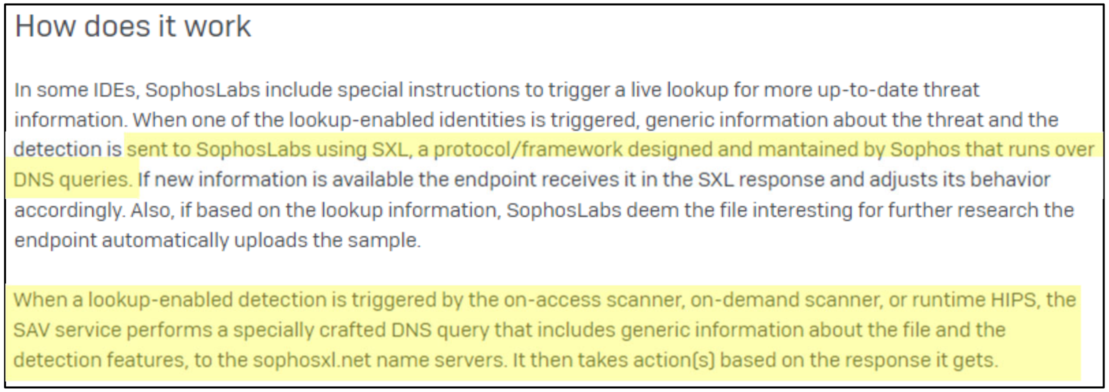
2. To change when on-access scanning occurs, under **Check files on**, set the options as described below.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Read</td><td>Scan files when they are copied, moved, or opened.</td></tr>
<tr><td>Rename</td><td>Scan files when they are renamed.</td></tr>
<tr><td>Write</td><td>Scan files when they are saved or created.</td></tr>
</table>

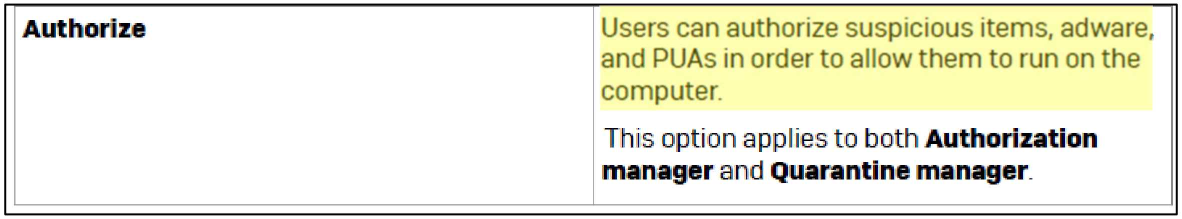
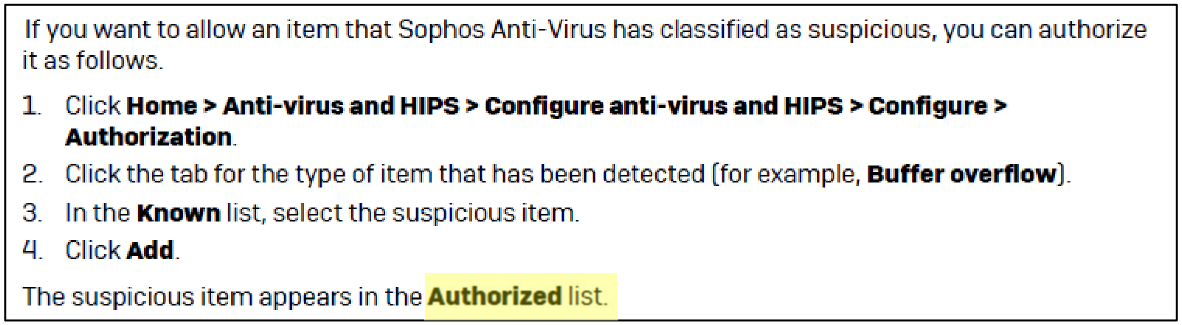
https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf, at pp. 7-8

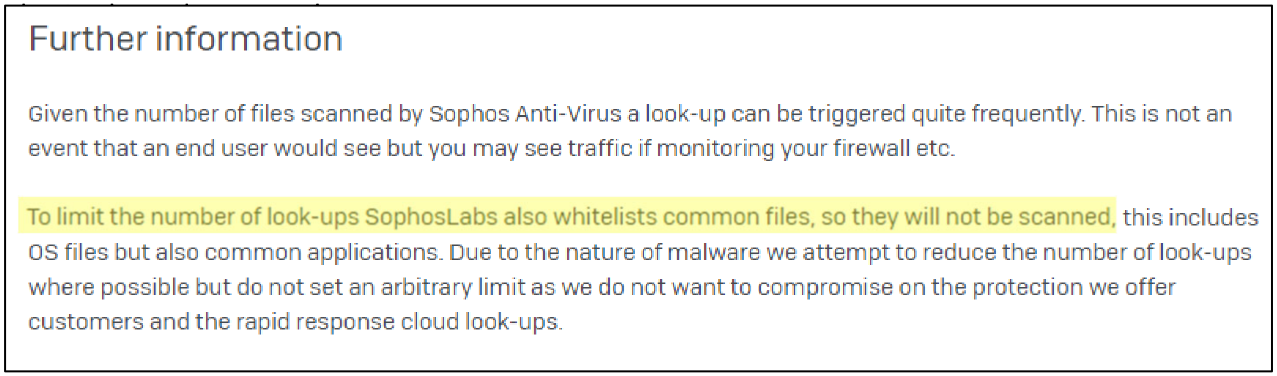
</td></tr>
</table>

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

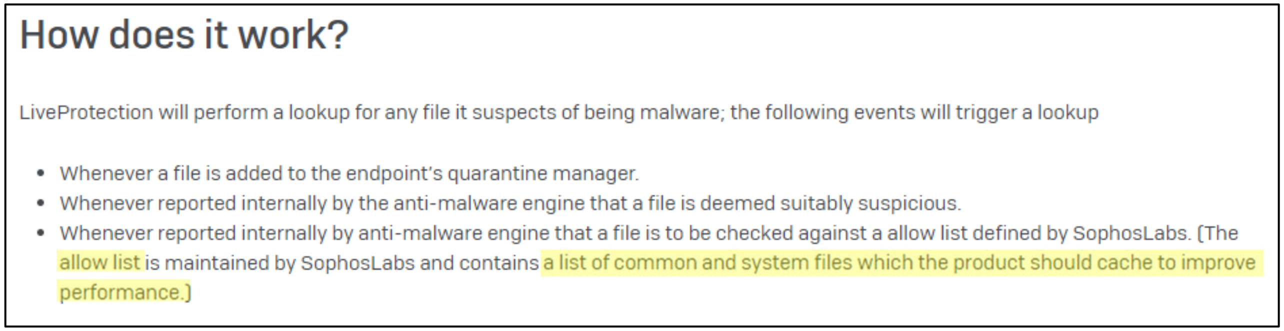
CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	In response to the "malicious and suspicious behavior detection" and/or "on-access scanning" discussed in the previous two slides, the Sophos software on the computer sends the request for permission value (e.g., a Live Protection lookup query).  • **Enable Live Protection** If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis. The in-the-cloud checking performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf, at p. 28  How does it work In some IDEs, SophosLabs include special instructions to trigger a live lookup for more up-to-date threat information. When one of the lookup-enabled identities is triggered, generic information about the threat and the detection is sent to SophosLabs using SXL, a protocol/framework designed and mantained by Sophos that runs over DNS queries. If new information is available the endpoint receives it in the SXL response and adjusts its behavior accordingly. Also, if based on the lookup information, SophosLabs deem the file interesting for further research the endpoint automatically uploads the sample. When a lookup-enabled detection is triggered by the on-access scanner, on-demand scanner, or runtime HIPS, the SAV service performs a specially crafted DNS query that includes generic information about the file and the detection features, to the sophosxl.net name servers. It then takes action(s) based on the response it gets. https://community.sophos.com/kb/en-us/111334

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

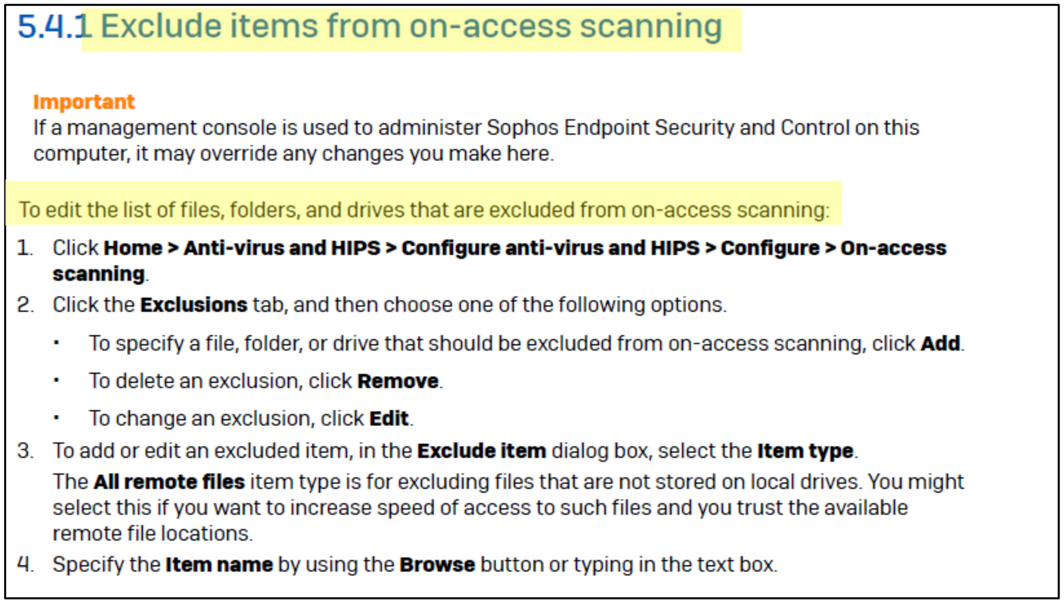
CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Sophos's software interrogates a local database of permission values to locate a permission value associated with the application in the local database. This includes interrogating databases populated by Sophos permission values or by permission values set by the user. For example, the Sophos software utilizes rules, policies, whitelists, authorized lists, and/or exceptions that are stored in a local database. For example, Sophos's "Authorized list" includes at lease one permission value (e.g., an authorization) associated with each item on the list, and each item is associated with an application. If it fails to locate a permission value associated with the application from the Authorized list in the local database, and fails to identify whether the application is clean or malicious using locally stored information on the computer, it sends a query to the SophosLabs network.  **Authorize** — Users can authorize suspicious items, adware, and PUAs in order to allow them to run on the computer. This option applies to both **Authorization manager** and **Quarantine manager**.  If you want to allow an item that Sophos Anti-Virus has classified as suspicious, you can authorize it as follows. 1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Authorization**. 2. Click the tab for the type of item that has been detected (for example, **Buffer overflow**). 3. In the **Known** list, select the suspicious item. 4. Click **Add**. The suspicious item appears in the **Authorized** list. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf, at pp. 6, 32

CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	As another example, Sophos's software includes "whitelists" stored in a local database of the computer to limit the number of Live Protection lookups. The whitelists includes at least one permission value (e.g., an authorization) associated with each item on the list, and each item is associated with an application. If the Sophos software fails to locate a permission value associated with the application from the whitelist in the local database, and fails to identify whether the application is clean or malicious using locally stored information on the computer, it sends a query to  Further information Given the number of files scanned by Sophos Anti-Virus a look-up can be triggered quite frequently. This is not an event that an end user would see but you may see traffic if monitoring your firewall etc. To limit the number of look-ups SophosLabs also whitelists common files, so they will not be scanned, this includes OS files but also common applications. Due to the nature of malware we attempt to reduce the number of look-ups where possible but do not set an arbitrary limit as we do not want to compromise on the protection we offer customers and the rapid response cloud look-ups. https://community.sophos.com/kb/en-us/111334

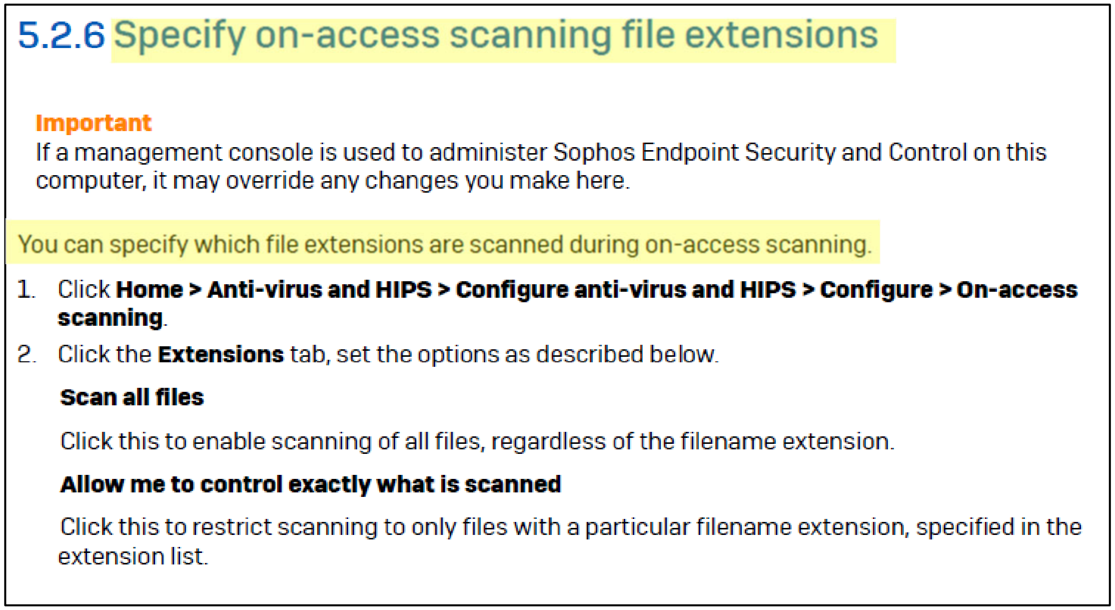
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

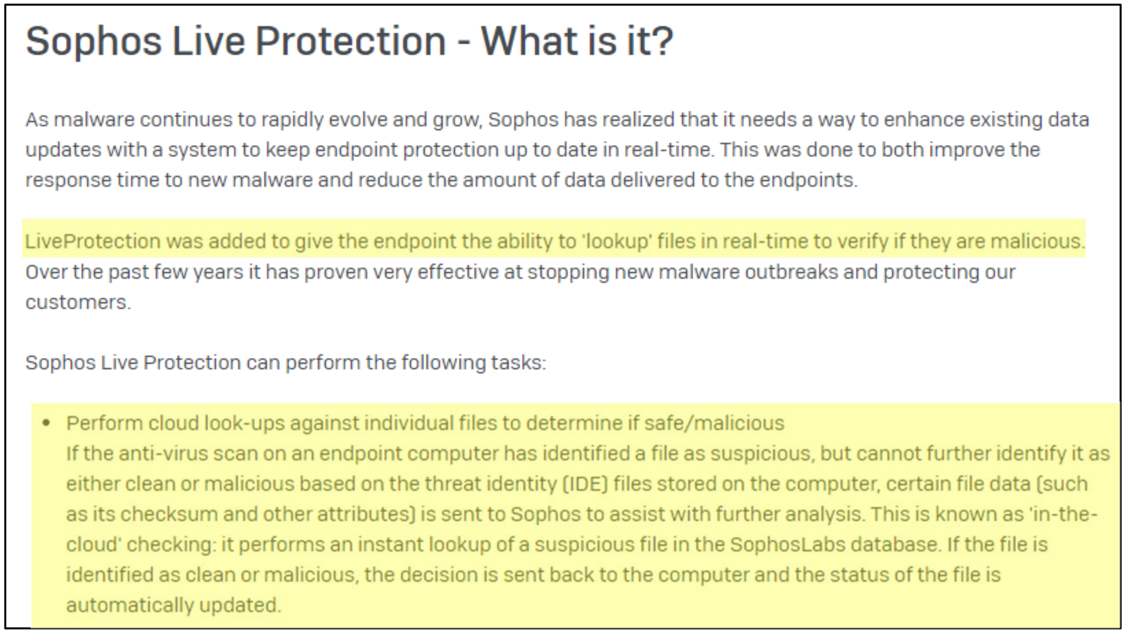
CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	As another example, Sophos's software includes an allow list. The allow list includes at least one permission value (e.g., an authorization) associated with each item on the list, and each item is associated with an application. If the Sophos software fails to locate a permission value associated with the application from the allow list in the local database, and fails to identify whether the application is clean or malicious using locally stored information on the computer, it sends a query to the SophosLabs network. While an allow list is maintained by SophosLabs, the list is provided to and stored in the computer to "improve performance."  How does it work? LiveProtection will perform a lookup for any file it suspects of being malware; the following events will trigger a lookup • Whenever a file is added to the endpoint's quarantine manager. • Whenever reported internally by the anti-malware engine that a file is deemed suitably suspicious. • Whenever reported internally by anti-malware engine that a file is to be checked against a allow list defined by SophosLabs. (The allow list is maintained by SophosLabs and contains a list of common and system files which the product should cache to improve performance.) https://community.sophos.com/kb/en-us/110921

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	As another example, Sophos's software uses excluded lists stored in a local database of the computer. The excluded lists use at least one permission value (e.g., an authorization) associated with each item on the list, and each item is associated with an application. If the Sophos software fails to locate a permission value associated with the application from the excluded list in the local database, and fails to identify whether the application is clean or malicious using locally stored information on the computer, it sends a query to the SophosLabs network.  5.4.1 Exclude items from on-access scanning **Important** If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here. To edit the list of files, folders, and drives that are excluded from on-access scanning: 1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning**. 2. Click the **Exclusions** tab, and then choose one of the following options. • To specify a file, folder, or drive that should be excluded from on-access scanning, click **Add**. • To delete an exclusion, click **Remove**. • To change an exclusion, click **Edit**. 3. To add or edit an excluded item, in the **Exclude item** dialog box, select the **Item type**. The **All remote files** item type is for excluding files that are not stored on local drives. You might select this if you want to increase speed of access to such files and you trust the available remote file locations. 4. Specify the **Item name** by using the **Browse** button or typing in the text box. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf, at p. 21

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	As another example, Sophos's software uses specified file extensions stored in a local database of the computer. The specified file extension are at least one permission value (e.g., a directive to scan) associated with each item on the list, and each item is associated with an application. If the Sophos software locates a permission value associated with the application from the file extension list in the local database, but fails to identify whether the application is clean or malicious using locally stored information on the computer, it sends a query to the SophosLabs network.  5.2.6 Specify on-access scanning file extensions **Important** If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here. You can specify which file extensions are scanned during on-access scanning. 1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning**. 2. Click the **Extensions** tab, set the options as described below. **Scan all files** Click this to enable scanning of all files, regardless of the filename extension. **Allow me to control exactly what is scanned** Click this to restrict scanning to only files with a particular filename extension, specified in the extension list. https://docs.sophos.com/esg/endpoint-security-and-control/10-6/help/en-us/PDF/sesc_h.pdf, at p. 11

CLAIM 29	SOPHOS PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	As yet another example, Sophos's "threat identity (IDE)" files are stored in a local database of the computer. The IDE files include at least one permission value (e.g., indicating whether the item is malicious or if the maliciousness of the item is known) associated with each item on the list, and each item is associated with an application. If the Sophos software fails to locate a permission value associated with the application from the threat identities in the local database, it sends a query to the SophosLabs network.  Sophos Live Protection - What is it? As malware continues to rapidly evolve and grow, Sophos has realized that it needs a way to enhance existing data updates with a system to keep endpoint protection up to date in real-time. This was done to both improve the response time to new malware and reduce the amount of data delivered to the endpoints. LiveProtection was added to give the endpoint the ability to 'lookup' files in real-time to verify if they are malicious. Over the past few years it has proven very effective at stopping new malware outbreaks and protecting our customers. Sophos Live Protection can perform the following tasks: • Perform cloud look-ups against individual files to determine if safe/malicious If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis. This is known as 'in-the-cloud' checking: it performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated. https://community.sophos.com/kb/en-us/110921

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	SOPHOS PRODUCTS
29[e] selecting the stored permission value in response to receiving the request; and **29[f] transmitting to said first computer the output permission value derived from the plurality of received permission values to the first computer over the data network in order to cause the monitoring process operating on the first computer to permit or deny write access by the application to the data storage device in dependence on the transmitted output permission value.**	For the SophosLabs network to respond to a query or update a local database (e.g., a locally stored whitelist or IDE file), it must select the stored permission value in response to receiving the request and transmit it to the first computer. The output permission value is derived from the plurality of received permission values as discussed for limitation 29[c]. That response is sent to cause the Sophos software operating on the first computer to permit or deny write access by the application to the data storage device in dependence on the transmitted output permission value. As discussed previously, the purpose of the SophosLabs network is to provide the first computer with the latest threat information. And as discussed previously, that information is used to determine whether to allow or deny write access to the application. The slides related to limitation 29[b] and [c] are incorporated herein.